IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	:	
Natsume MATSUZAKI et al.	:	
Serial No. NEW	:	**Attn: APPLICATION BRANCH**
Filed August 28, 2003	:	**Attorney Docket No. 2003_1213A**
GROUP FORMATION/MANAGEMENT SYSTEM, GROUP MANAGEMENT DEVICE, AND MEMBER DEVICE	:	

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEES FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-260520, filed September 5, 2002, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Natsume MATSUZAKI et al.

By _____
Jeffrey R. Filipek
Registration No. 41,471
Attorney for Applicants

JRF/fs
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
August 28, 2003

日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年　９月　５日

出願番号
Application Number:　特願２００２－２６０５２０

[ST.10/C]:　[ＪＰ２００２－２６０５２０]

出願人
Applicant(s):　松下電器産業株式会社

２００３年　５月２０日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０３７４７７

【書類名】　特許願

【整理番号】　2022540350

【提出日】　平成14年 9月 5日

【あて先】　特許庁長官　殿

【国際特許分類】　G11B 20/10

G09C 1/00

G06F 12/14

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　松崎　なつめ

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　阿部　敏久

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　中野　稔久

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　布田　裕一

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　宮▲ざき▼　雅也

【特許出願人】

【識別番号】　000005821

出証特２００３－３０３７４７７

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100090446

【弁理士】

【氏名又は名称】　中島　司朗

【手数料の表示】

【予納台帳番号】　014823

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9003742

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】グループ情報システムおよび認証通信プロトコルおよび端末

【特許請求の範囲】

【請求項１】　グループ管理端末が、グループメンバー端末を登録し、その結果共通秘密情報を共有するグループ情報システムであって、グループ管理端末は、グループ全体の登録端末の台数を管理する台数制御部と、共通秘密情報配布部を含み、グループメンバー端末は、グループ管理端末より配布された共通秘密情報を格納する共通秘密情報格納部を含んでおり、グループ管理端末は、台数制御部の制御に従って、共通秘密鍵配布部が共通秘密情報を前記グループメンバー端末に配布して、台数制御部が登録台数を更新し、一方、グループメンバー端末の共通秘密情報格納部は、送付された共通秘密情報を蓄積することを特徴とするグループ情報システム。

【請求項２】　前記グループ管理端末とグループメンバー端末はネットワークを介して接続されており、前記グループ管理端末は、前記グループメンバー端末の正当性を、ネットワークを介して確認してセッション鍵を共有し、前記セッション鍵で前記共通秘密情報を暗号化して配布し、前記グループメンバー端末は、前記グループ管理端末からネットワークを介して配布されたデータを、共有されたセッション鍵で復号し、その結果得た共通秘密情報を、前記共通秘密情報格納部に格納することを特徴とする、請求項１記載のグループ情報システム。

【請求項３】　前記グループメンバー端末とグループメンバー端末が、オフラインであることを特徴とする、請求項１記載のグループ情報システム。

【請求項４】　前記グループメンバー端末があらかじめ共通秘密情報を有している場合には、グループ管理端末は、共通秘密情報の配布をせずに処理を終了することを特徴とする、請求項１記載のグループ情報システム。

【請求項５】　共通秘密情報を有した第1のグループメンバー端末が、第2のグループメンバー端末に前記共通秘密情報を転送するグループ情報システムであって、前記第1のグループメンバー端末は、共通秘密情報を格納している共通秘密情報格納部と、第2のグループメンバー端末に前記共通秘密情報を転送する共通秘密情報転送部と、その後共通秘密情報を消去制御する共通秘密情報消去制御部

を含み、前記第2のグループメンバー端末は、第1のグループメンバー端末から転送された共通秘密情報を格納する共通秘密情報格納部と、共通秘密情報書き込み制御部を含んでおり、前記第1のグループメンバー端末の共通秘密情報転送部は、共通秘密情報格納部にある共通秘密情報を前記第2のグループメンバー端末に転送し、その後共通秘密情報消去制御部が共通秘密情報を消去し、一方、第2のグループメンバー端末は第1のグループメンバー端末から受信した共通秘密情報を前記共通秘密情報格納部に書き込むことを特徴とするグループ情報システム。

【請求項６】　前記第2のグループメンバー端末があらかじめ共通秘密情報を有している場合には、第1のグループメンバー端末は、共通秘密情報の転送をせずに処理を終了することを特徴とする、請求項５記載のグループ情報システム。

【請求項７】　グループ管理端末が、グループメンバー端末の登録を削除するグループ情報システムであって、グループ管理端末は、グループメンバーが共通秘密情報を保有していることを確認する共通秘密情報確認部と、登録グループメンバー端末の台数を管理する台数制御部を含み、グループメンバー端末は、共通秘密情報格納部と、共通秘密情報を保有していることを証明する共通秘密情報証明部と、共通秘密情報消去制御部を含んでおり、前記グループメンバー端末の登録削除要求で、グループ管理端末の共通秘密情報格納部が、グループメンバー端末が共通秘密情報を保持していることを確認した後、グループメンバー端末は共通秘密情報を削除し、一方、グループ管理端末の台数制御部は登録台数を更新するグループ情報システム。

【請求項８】　前記グループ管理端末あるいは各グループメンバー端末は個別の識別子を保持しており、登録、転送、登録削除の際に、相手認証を行い、あらかじめ配布されているリボケーション端末リストを参照して、端末識別子が、リストにある場合は、登録、転送、登録削除の処理を行わないことを特徴とする請求項１、５、７のいずれかに記載のグループ情報システム。

【請求項９】　前記リボケーション端末リストには、信頼の置けるセンターの署名が付加されており、パッケージ化されたメディア、あるいは放送、あるいはネットワークを介して配布されることを特徴とする請求項８記載のグループ情報システム。

【請求項１０】　前記共通秘密情報は、グループ管理端末が任意に生成して管理することを特徴とする請求項１、５、７のいずれかに記載のグループ情報システム。

【請求項１１】　前記共通秘密情報は、別に設けた信頼の置けるセンターにて生成され、管理され、前記グループ管理端末に通知されることを特徴とする請求項１、５、７のいずれかに記載のグループ情報システム。

【請求項１２】　前記共通秘密情報は、定期的あるいは不定期に更新することを特徴とする請求項１、５、７のいずれかに記載のグループ情報システム。

【請求項１３】　前記グループ管理端末が管理するグループメンバー端末の制限台数は、別に設けた信頼の置けるセンターにて管理し、前記グループ管理端末に通知されることを特徴とする請求項１、５、７のいずれかに記載のグループ情報システム。

【請求項１４】　前記グループ管理端末が管理するグループメンバー端末の制限台数に対応して、別に設けた課金システムがグループに送付するデータに課金することを特徴とする請求項１、５、７のいずれかに記載のグループ情報システム。

【請求項１５】　前記グループ管理端末が管理するグループメンバー端末の制限台数において、オンラインのグループメンバー機器の台数と、オフラインのグループメンバー機器の台数を個々に定めることを特徴とする請求項１、５、７のいずれかに記載のグループ情報システム。

【請求項１６】　前記グループ管理端末が管理するグループメンバー端末の制限台数において、オンラインのグループメンバー機器の台数と、オフラインのグループメンバー機器の台数の合計を定めることを特徴とする請求項１、５、７のいずれかに記載のグループ情報システム。

【請求項１７】　前記グループ管理端末とグループメンバー端末の間で、共通の時刻情報を保持し、また有効期限を定め、その有効期限の間だけグループメンバー端末はグループ管理端末から共有秘密情報を移動し、有効期限が終了したら、共有秘密情報を削除して、一方前記グループ管理端末は登録情報をもとに戻すことを特徴する請求項１記載のグループ情報システム。

【請求項１８】　前記第1のグループメンバー端末と第2のグループメンバー端末の間で、共通の時刻情報を保持し、また有効期限を定め、その有効期限の間だけ第２のグループメンバー端末は第1のグループメンバー端末から共有秘密情報を移動し、有効期限が終了したら、共有秘密情報を削除して、一方第1のグループメンバー端末は共通秘密情報を復活することを特徴する請求項５記載のグループ情報システム。

【請求項１９】　前記グループメンバー端末は、複数の前記グループ管理端末の中から、距離や通信時間、処理能力、処理状態に依存して、１つのグループ管理端末を選んで登録要求、または前記共通秘密情報の転送要求を行うことを特徴とする請求項１、５のいずれかに記載のグループ情報システム。

【請求項２０】　前記グループ秘密情報は、複数の前記グループ管理端末および、各グループ管理端末に登録されているグループメンバー端末間で、総合計の登録台数以内で、秘密に共有することを特徴とする請求項１、５、７のいずれかに記載のグループ情報システム。

【請求項２１】　前記請求項１または５において、前記グループメンバー端末に、共通秘密情報が未設定であることを確認し、セッション鍵を共有する認証通信プロトコル。

【請求項２２】　前記請求項７において、前記グループメンバー端末に、共通の前記共通秘密情報が設定されていることを確認し、セッション鍵を共有する認証通信プロトコル。

【請求項２３】　請求項１、５、７のいずれかに記載のグループ情報システムにおける、グループ管理端末。

【請求項２４】　前記グループ管理端末の、少なくとも、台数制御部および共通秘密情報は、許可なく書き込み、読み出し、コピーができない領域に実装することを特徴とする、前記請求項２３記載のグループ管理端末。

【請求項２５】　前記許可なく書き込み、読み出し、コピーができない領域を、着脱可能なデバイスに実装することを特徴とする、前記請求項２４記載のグループ管理端末。

【請求項２６】　請求項１、５、７のいずれかに記載のグループ情報システム

における、グループメンバー端末。

【請求項２７】　前記グループメンバー端末の、少なくとも、共通秘密情報格納部は、許可なく、書き込み、読み出し、コピーができない領域に実装することを特徴とする、請求項２６記載のグループメンバー端末。

【請求項２８】　前記許可なく書き込み、読み出し、コピーができない領域を、着脱可能なデバイスに実装することを特徴とする、請求項２７記載のグループメンバー端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ディジタルコンテンツのコピーや移動が相互に可能なグループを形成、管理するグループ情報システムに関する。

【０００２】

【従来の技術】

近年、音楽や映像、ゲームなどデジタルコンテンツはインターネットやデジタル放送および、パッケージメディアによる流通により容易に取得が可能となってきている。

このようなシステムでは、通常、コンテンツの著作権を保護するために、コンテンツは暗号化され、それを獲得する権利のある機器だけが復号できるようになっている。例えば、インターネットを用いたデジタルコンテンツの配布では、配布元であるサーバと、コンテンツを利用するクライアント機器の間で認証が行われ、サーバは予め登録されたクライアント機器であることを確認後、コンテンツをそのクライアント機器だけが有する鍵を用いて暗号化して配布する。

【０００３】

以下に、サーバとクライアント機器間の認証方法の一例として、公開鍵暗号を用いた相手認証方法を示す（例えば、非特許文献１参照）。

第1の機器が第2の機器にチャレンジデータとして乱数データを送信し、続いて、第2の機器がその乱数データに対して自分の秘密鍵で暗号化（電子署名など）して第1の機器にレスポンスデータを返信し、最後に、返信されてきた暗号文（

あるいは、署名文）に対して、第1の機器が第2の機器の公開鍵を用いて検証するというものがある。一般に、このような公開鍵暗号を用いた認証においては、公開鍵そのものが有効であることが前提となる。

【０００４】

このために、認証局と呼ばれる機関から、各機器に対応する正しい公開鍵であることを示す（公開鍵に対する「お墨付き」となる）「公開鍵証明書」が発行されることが一般的である。公開鍵証明書は、機器の識別名や有効期限と公開鍵を結合したデータに認証局の電子署名が付与されたものであり、これを受け取った機器は、その電子署名の正しさを確認し、さらに通信機器の識別名や現在の時間からその公開鍵証明書の記載内容を確認した上で、公開鍵の正しさを確認するものである。さらに、発行された公開鍵証明書のうち、不正を働いた機器、あるいは秘密鍵が盗まれた機器の公開鍵証明書については、それらが無効化されていることを他の機器に知らせるために、無効化した公開鍵証明書を特定する情報の一覧に対して認証局の電子署名が付与された公開鍵証明書無効化リスト（Certificate Revocation List：以下、ＣＲＬ）として発行される（例えば、非特許文献２参照）。

【０００５】

このように、相手機器の公開鍵を用いてその相手機器を認証する際には、その相手機器から公開鍵証明書を入手し、入手した公開鍵証明書がCRLに登録されたもの（無効化されたもの）でないことを確認する。

上記サーバとクライアント機器によるコンテンツ配布のモデルによれば、コンテンツを利用したいすべてのクライアント機器は、サーバと接続する必要があり、また上記に述べた公開鍵暗号を用いた相手認証を行う場合は、その仕組みを備える必要がある。これは家庭内の機器全体を考えたときには、クライアント機器となる機器（コンテンツを扱うことができる機器）の能力を限定することにもなる。またサーバにおいても、すべてのクライアント機器を管理する必要がある。

以上のことにより、サーバと接続できるクライアント機器から、さらに「ある許可された範囲」の機器にコンテンツを再配布する階層的なモデルが考えられる。本発明では、この「ある許可された範囲」の規定と管理の仕方、およびその範囲

でのコンテンツの配布方法について対象とする。なお、以降では、「ある許可された範囲」を「AD（Authorized Domainの略）」あるいはより一般的には「グループ」と呼び、AD内にあり、サーバと接続できるクライアント機器を「AD内サーバ」、AD内サーバ以外の機器を「AD内クライアント」と呼ぶことにする。

【０００６】

AD内サーバとAD内クライアントの間のコンテンツ保護技術として用いることができるものの１つに、DTCP（Digital Transmission Content Protection）と呼ばれる規格がある（例えば、非特許文献３参照）。

DTCPは高速シリアルバス規格の１つのIEEE1394を介して配信されるディジタルコンテンツの保護規格である。DTCPでは、DTLA（Digital Transmission Licensing Administrator, LLC）と呼ばれる管理者の管理の下でDTCP規格に準拠した機器を相互接続し、その間で暗号認証通信を行っている。その仕組みの概要は次のとおりである。

【０００７】

(1)送信機器および受信機器（上記の、AD内サーバとAD内クライアントにそれぞれ対応）は、それぞれDTLAから配布された秘密鍵を備えている。この秘密鍵の配布はDTLAとの契約に基づいて各機器に配布される。

(2)送信機器と受信機器は、上記秘密鍵を用いて相互認証する。また、送信機器は、コンテンツ保護が必要となるコンテンツを、認証により共有した鍵で暗号化して送信する。

【０００８】

(3)送信機器は、最大63台までの受信機器にコンテンツを復号するための鍵を与える。

つまり、DTCPは、コンテンツを利用するたびに定まる最大63台をADとして、AD内での視聴を許可している。

【０００９】

【非特許文献１】

岡本龍明、山本博資、”現代暗号”、産業図書（1997年）、１５５ページ～１５６ページ

【００１０】

【非特許文献２】

American National Standards Institute, American National Standard for Financial Services, ANSX9.57: Public Key Cryptography For the Financial Industry: Certificate Management, 1997.

【００１１】

【非特許文献３】

DTCP SpecificationのWhite paper ＜URL： HYPERLINK "http://www.dtcp.com/spec.html" http://www.dtcp.com/spec.html＞

【００１２】

【非特許文献４】

池野信一、小山謙二、「現代暗号理論」、電子通信学会、１７５ページ～１７７ページ

【００１３】

【発明が解決しようとする課題】

上記述べたDTCPでは、次の課題がある。

(1) DTCPではコンテンツを利用するたびにADがダイナミックに設定される。しかし、著作権保護の観点からは、より固定的なADのほうが望ましい。

(2) DTCPでは AD内の機器台数が、最大63台と決まっているが、より柔軟で、AD内の機器台数に依存した課金も可能であるシステムが望ましい。

【００１４】

(3) DTCPでは、AD内での視聴が許可されるが、AD内でのコピーも可能となるような、拡張が望ましい。

(4) DTCPでは視聴のたびに、AD内クライアントはAD内サーバに接続する必要があるが、ネットワークを介さないAD内クライアントでのコンテンツの利用も可能であるのが望ましい。

【００１５】

本発明では、以上のことを鑑み、次の条件を満たす情報システムと端末を提供することを目的とする。

・ADサーバがAD内のクライアント台数を管理し、この範囲でのコンテンツの利用、コピー等を可能とする。AD内の機器の登録や脱退、機器の変更を可能とする。

【００１６】

・AD内の登録機器台数は、柔軟に管理、運用する。AD内の登録機器台数に依存した課金も可能とする。

・AD内サーバとオンライン接続されていない機器（例えば車載機器など）もAD内クライアントとして登録が可能とする。このために、例えばICカードのような着脱可能なセキュアデバイスを利用する。

【００１７】

【課題を解決するための手段】

請求項1による本発明のグループ情報システムは、

グループ管理端末が、グループメンバー端末を登録し、その結果共通秘密情報を共有するグループ情報システムであって、グループ管理端末は、グループ全体の登録端末の台数を管理する台数制御部と、共通秘密情報配布部を含み、グループメンバー端末は、グループ管理端末より配布された共通秘密情報を格納する共通秘密情報格納部を含んでおり、グループ管理端末は、台数制御部の制御に従って、共通秘密鍵配布部が共通秘密情報を前記グループメンバー端末に配布して、台数制御部が登録台数を更新し、一方、グループメンバー端末の共通秘密情報格納部は、送付された共通秘密情報を蓄積することを特徴とする。

【００１８】

請求項２による本発明のグループ情報システムは、請求項１における前記グループ管理端末とグループメンバー端末はネットワークを介して接続されており、前記グループ管理端末は、前記グループメンバー端末の正当性を、ネットワークを介して確認してセッション鍵を共有し、前記セッション鍵で前記共通秘密情報を暗号化して配布し、前記グループメンバー端末は、前記グループ管理端末からネットワークを介して配布されたデータを、共有されたセッション鍵で復号し、その結果得た共通秘密情報を、前記共通秘密情報格納部に格納することを特徴とする。

【００１９】

請求項３による本発明のグループ情報システムは、請求項１における前記グループメンバー端末とグループメンバー端末が、オフラインであることを特徴とする。

請求項４による本発明のグループ情報システムは、請求項１における前記グループメンバー端末があらかじめ共通秘密情報を有している場合には、グループ管理端末は、共通秘密情報の配布をせずに処理を終了することを特徴とする。

【００２０】

請求項５による本発明のグループ情報システムは、共通秘密情報を有した第1のグループメンバー端末が、第2のグループメンバー端末に前記共通秘密情報を転送するグループ情報システムであって、前記第1のグループメンバー端末は、共通秘密情報を格納している共通秘密情報格納部と、第2のグループメンバー端末に前記共通秘密情報を転送する共通秘密情報転送部と、その後共通秘密情報を消去制御する共通秘密情報消去制御部を含み、前記第2のグループメンバー端末は、第1のグループメンバー端末から転送された共通秘密情報を格納する共通秘密情報格納部と、共通秘密情報書き込み制御部を含んでおり、前記第1のグループメンバー端末の共通秘密情報転送部は、共通秘密情報格納部にある共通秘密情報を前記第2のグループメンバー端末に転送し、その後共通秘密情報消去制御部が共通秘密情報を消去し、一方、第2のグループメンバー端末は第1のグループメンバー端末から受信した共通秘密情報を前記共通秘密情報格納部に書き込むことを特徴とする。

【００２１】

請求項６による本発明のグループ情報システムは、請求項５における前記第2のグループメンバー端末があらかじめ共通秘密情報を有している場合には、第1のグループメンバー端末は、共通秘密情報の転送をせずに処理を終了することを特徴とする。

請求項７による本発明のグループ情報システムは、グループ管理端末が、グループメンバー端末の登録を削除するグループ情報システムであって、グループ管理端末は、グループメンバーが共通秘密情報を保有していることを確認する共通

秘密情報確認部と、登録グループメンバー端末の台数を管理する台数制御部を含み、グループメンバー端末は、共通秘密情報格納部と、共通秘密情報を保有していることを証明する共通秘密情報証明部と、共通秘密情報消去制御部を含んでおり、前記グループメンバー端末の登録削除要求で、グループ管理端末の共通秘密情報格納部が、グループメンバー端末が共通秘密情報を保持していることを確認した後、グループメンバー端末は共通秘密情報を削除し、一方、グループ管理端末の台数制御部は登録台数を更新することを特徴とする。

【００２２】

請求項８による本発明のグループ情報システムは、請求項１、５、７のいずれかにおける前記グループ管理端末あるいは各グループメンバー端末は個別の識別子を保持しており、登録、転送、登録削除の際に、相手認証を行い、あらかじめ配布されているリボケーション端末リストを参照して、端末識別子が、リストにある場合は、登録、転送、登録削除の処理を行わないことを特徴とする。

【００２３】

請求項９による本発明のグループ情報システムは、請求項８における、前記リボケーション端末リストには、信頼の置けるセンターの署名が付加されており、パッケージ化されたメディア、あるいは放送、あるいはネットワークを介して配布されることを特徴とする。

請求項１０による本発明のグループ情報システムは、請求項１、５、７のいずれかにおける、前記共通秘密情報は、グループ管理端末が任意に生成して管理することを特徴とする。

【００２４】

請求項１１による本発明のグループ情報システムは、請求項１、５、７のいずれかにおける、前記共通秘密情報は、別に設けた信頼の置けるセンターにて生成され、管理され、前記グループ管理端末に通知されることを特徴とする。

請求項１２による本発明のグループ情報システムは、請求項１、５、７のいずれかにおける、

前記共通秘密情報は、定期的あるいは不定期に更新することを特徴とする。

【００２５】

請求項１３による本発明のグループ情報システムは、請求項１、５、７のいずれかにおける、

前記グループ管理端末が管理するグループメンバー端末の制限台数は、別に設けた信頼の置けるセンターにて管理し、前記グループ管理端末に通知されることを特徴とする。

【００２６】

請求項１４による本発明のグループ情報システムは、請求項１、５、７のいずれかにおける、前記グループ管理端末が管理するグループメンバー端末の制限台数に対応して、別に設けた課金システムがグループに送付するデータに課金することを特徴とする。

請求項１５による本発明のグループ情報システムは、請求項１、５、７のいずれかにおける、前記グループ管理端末が管理するグループメンバー端末の制限台数において、オンラインのグループメンバー機器の台数と、オフラインのグループメンバー機器の台数を個々に定めることを特徴とする。

【００２７】

請求項１６による本発明のグループ情報システムは、請求項１、５、７のいずれかにおける、前記グループ管理端末が管理するグループメンバー端末の制限台数において、オンラインのグループメンバー機器の台数と、オフラインのグループメンバー機器の台数の合計を定めることを特徴とする。

請求項１７による本発明のグループ情報システムは、請求項１における、前記グループ管理端末とグループメンバー端末の間で、共通の時刻情報を保持し、また有効期限を定め、その有効期限の間だけグループメンバー端末はグループ管理端末から共有秘密情報を移動し、有効期限が終了したら、共有秘密情報を削除して、一方前記グループ管理端末は登録情報をもとに戻すことを特徴する。

【００２８】

請求項１８による本発明のグループ情報システムは、請求項５における、前記第1のグループメンバー端末と第2のグループメンバー端末の間で、共通の時刻情報を保持し、また有効期限を定め、その有効期限の間だけ第２のグループメンバー端末は第1のグループメンバー端末から共有秘密情報を移動し、有効期限が終

了したら、共有秘密情報を削除して、一方第1のグループメンバー端末は共通秘密情報を復活することを特徴する。

【００２９】

請求項１９による本発明のグループ情報システムは、請求項１、５のいずれかにおける、前記グループメンバー端末は、複数の前記グループ管理端末の中から、距離や通信時間、処理能力、処理状態に依存して、１つのグループ管理端末を選んで登録要求、または前記共通秘密情報の転送要求を行うことを特徴とする。

請求項２０による本発明のグループ情報システムは、請求項１、５、７のいずれかにおける、前記グループ秘密情報は、複数の前記グループ管理端末および、各グループ管理端末に登録されているグループメンバー端末間で、総合計の登録台数以内で、秘密に共有することを特徴とする。

【００３０】

請求項２１による本発明の認証通信プロトコルは、前記請求項１、５のいずれかにおいて、前記グループメンバー端末に、共通秘密情報が未設定であることを確認し、セッション鍵を共有することを特徴とする。

請求項２２による本発明の認証通信プロトコルは、前記請求項７において、前記グループメンバー端末に、共通の前記共通秘密情報が設定されていることを確認し、セッション鍵を共有することを特徴とする。

【００３１】

請求項２３による本発明のグループ管理端末は、前記請求項１、５、７のいずれかに記載のグループ情報システムにおける、グループ管理端末である。

請求項２４による本発明のグループ管理端末は、請求項２３における前記グループ管理端末の、少なくとも、台数制御部および共通秘密情報は、許可なく書き込み、読み出し、コピーができない領域に実装することを特徴とする。

【００３２】

請求項２５による本発明のグループ管理端末は、請求項２４における前記許可なく書き込み、読み出し、コピーができない領域を、着脱可能なデバイスに実装することを特徴とする。

請求項２６による本発明のグループメンバー端末は、前記請求項１、５、７の

いずれかに記載のグループ情報システムにおける、グループメンバー端末である。

【００３３】

請求項２７による本発明のグループメンバー端末は、請求項２６における、前記グループメンバー端末の、少なくとも、共通秘密情報格納部は、許可なく、書き込み、読み出し、コピーができない領域に実装することを特徴とする

請求項２７による本発明のグループメンバー端末は、請求項２７における、前記許可なく書き込み、読み出し、コピーができない領域を、着脱可能なデバイスに実装することを特徴とする。

【００３４】

【発明の実施の形態】

＜ADの概念説明＞

図1は、本発明の実施の形態に係る、ADの概念図である。

このADは、ADの登録台数を管理するAD内サーバ101と、1台以上のAD内クライアント（図では２台、111,112）からなる。AD内クライアントの中でも、111はAD内サーバとオンライン通信を介して接続しており、112はAD内サーバとオンライン接続はされていないものとする。同一AD内に含まれる機器の台数は、AD内サーバにより管理される。そして、同一AD内のAD内サーバ101、およびAD内クライアント111～112は、「共通秘密情報」（以下では、CSI（Common Secret Information）と称することもある）を共有している。このCSIは、各ADごとに異なるものとする。

【００３５】

同一AD内の任意の機器間、すなわち同じ「共通秘密情報」CSIを有する機器間では、AD内に送信されたあるいは、蓄積されたデジタルコンテンツの送受信や利用およびコピーが自由に行われる。

一方、AD外の機器であり同じCSIを保有していない機器120には、このAD内のデジタルコンテンツの送受信や利用、およびコピーが許可されない。

【００３６】

AD内サーバは、AD内の登録機器とその台数を管理する。

以下では、その管理方法の実施例とし、次の方法について順次説明を行う。

・ADへのクライアント機器の登録方法

・ADからクライアント機器の脱退方法

・クライアント機器間のCSIの移動方法

・AD内でのコンテンツ配布方法

＜ADへのクライアント機器の登録方法＞

［概念説明］

図２はAD内サーバへのクライアント機器の登録方法の概念を示したものである。

【００３７】

図２において、101はAD内サーバである。AD内サーバ101では、AD内の登録機器台数を管理し、予め決められている台数を限度として登録を許可する。ここでは例として2台とする。

AD内サーバに何も登録されていない状態から、まず、ネットワーク機能を有するクライアント機器111がオンライン通信を介して登録要求した場合、AD内サーバは登録台数を確認し、1台目なので登録処理を行う。登録処理ではAD内サーバは自身のデータベースに、登録情報としてクライアント機器111を登録して、AD内共通秘密情報CSIを送付する。次に2台目のクライアント機器112がオフラインで登録要求した場合も、2台目なので同様に登録処理を行う。オフラインでの登録では、例えば着脱可能なクライアント機器である場合には、AD内サーバの対応するスロットに装着する。あるいは、例えばAD内サーバが表示するCSIを、ユーザが直接クライアント機器に入力するという方法であってもよい。ただし、ユーザが入力する場合には、他の機器に勝手に同じCSIを入力されないよう、入力するコードはCSIを機器やセッションに依存して暗号化した値であるほうがよい。

【００３８】

次に、３台目のクライアント機器120がAD内サーバに登録要求したとき、すでに限度の2台を登録し、残りの登録可能台数が０なので、AD内サーバは登録処理を許可せずに処理を中継する。

［構成］

図３は、前記AD内サーバ101とクライアント機器111の内部構成を示している。

【００３９】

AD内サーバ101は、公開鍵暗号系における公開鍵に信頼できる第3者機関（CA: Certirication Authority と呼ぶ）の署名が付与された公開鍵証明書を格納する公開鍵証明書格納部201と、前記公開鍵に対応する秘密鍵を格納する秘密鍵格納部202と、公開鍵暗号の各種処理（署名生成／検証など）を実行する公開鍵暗号処理部203と、各クライアント機器に配布するAD内で共通の共通秘密情報を生成する共通秘密情報生成部211と、前記生成した共通秘密情報を格納する共通秘密情報格納部212と、登録情報を記憶する登録情報記憶部221と、共通秘密情報をクライアント機器に配布して登録処理をするか否かを判断する登録制御部222と、入出力部231を備える。

【００４０】

なお、ここで登録情報としては、例えば登録機器のIDや登録数の最大値、現在の登録数、残りの登録数とする。

一方、クライアント機器111は、公開鍵暗号系における公開鍵にCAの署名が付与された公開鍵証明書を格納する公開鍵証明書格納部241と、前記公開鍵に対応する秘密鍵を格納する秘密鍵格納部242と、公開鍵暗号の各種処理（署名生成／検証など）を実行する公開鍵暗号処理部243と、AD内サーバ101から配布された共通秘密鍵情報を格納する共通秘密情報格納部251と、入出力部261を備える。

【００４１】

ここで、少なくとも、AD内サーバの登録情報と、サーバおよびクライアント機器における秘密鍵、及び共通秘密情報は、外部に漏れることなく内部で厳重に管理される必要があるため、これらの情報は耐タンパ領域に格納されるものとする。

[動作フロー]

図４は、図３におけるクライアント機器111が、AD内サーバ101にAD登録する際の動作フローを示している。以下、その詳細について説明する。

【００４２】

S301：クライアント機器111がAD内サーバ101に登録要求を行う。この際、クラ

イアント機器は自身のID番号を通知する。

S302：AD内サーバ101とクライアント機器111の間で、公開鍵証明書を用いて公開鍵暗号における認証を行いセッション鍵を共有する。これにより、図３における入出力部231と261の間ではこのセッション鍵を用いた暗号通信が可能となる。暗号通信可能な通信路を、Secure Authentication Channel（SAC）と呼ぶ。具体的なSAC確立方法については後に述べる。

【００４３】

S303：AD内サーバは、クライアント機器111がすでに登録済みであるかを確認する。確認の方法としては、例えばAD内サーバの登録情報に前記クライアントのIDが含まれているかを確認するという方法がある。また、クライアント機器がすでに共通秘密情報CSIを保持しているかによっても確認することができる。もし、すでに登録されていれば、クライアント機器に登録済みである旨を通知して、AD内サーバは処理を中断する。

【００４４】

S304：AD内サーバは、登録情報記憶部に蓄積されている情報から、残りの登録数が０であるかを確認する。もし、０である場合は、これ以上は登録できないため、その旨をクライアント機器に通知して、処理を中断する。

S305：AD内サーバは、S302で共有したセッション鍵を用いて共通秘密情報CSIを暗号化し、クライアント機器に送付する。暗号文に追加してAD内サーバの署名を付加して送付してもよい。なお、最初のクライアント機器の登録時であって、もし前記共通秘密情報がなければ、図３における共通秘密情報生成部211において生成して、共通秘密情報格納部212に蓄積後、これを送付する。

【００４５】

S306：クライアント機器は、送付されたCSIを確認して共通秘密情報格納部に格納する。その後、AD内サーバに受領通知を送る。

S307：AD内サーバは、登録情報を更新する。具体的には、前記クライアントのIDを登録情報に追加して記録し、登録数のうち、現登録数を「＋１」、残り登録数を「－１」とする。

【００４６】

［ICカードで登録］

次に、クライアント機器がネットワーク機能を有さない、例えばICカードのような場合の登録について述べる。図５は、AD内サーバ101とICカード400の構成を示している。ただし、AD内サーバ101の構成要素は、図3に示す構成要素と同様として、ICカード400を挿入する挿入口450が追加されているものとする。

【００４７】

ICカード400は、公開鍵暗号系における公開鍵にCAの署名が付与された公開鍵証明書を格納する公開鍵証明書格納部401と、前記公開鍵に対応する秘密鍵を格納する秘密鍵格納部402と、公開鍵暗号の各種処理（署名生成／検証など）を実行する公開鍵暗号処理部403と、AD内サーバ101から配布された共通秘密情報を格納する共通秘密情報格納部411と、入出力部421を備える。

【００４８】

登録方法については、ICカード400をAD内サーバ101に挿入して、図4に示すフローと同様の方法で行えるため、その詳細については言及しない。なお、AD内サーバとICカードを密着して登録処理を行い、その間の不正がないと予測できる場合には、SACの確立は省略してもよい。

クライアント機器に、共通秘密情報が格納されたICカードが挿入されると、そのクライアント機器は、他のAD内のクライアント機器と同様に、AD内サーバ101が持つコンテンツ、あるいは他のクライアント機器が持つコンテンツを送受信することが可能となる。また、ICカードとAD未登録のクライアント機器の間で、後で述べる共通秘密情報の移動の処理を行いると、上記ICカードを介して、AD内サーバとはネットワークが接続されていないクライアント機器に共通秘密情報を設定することもできる。

【００４９】

なお、ICカードを利用したクライアント機器の登録方法において、ICカードに共通秘密情報を格納する場合、それを、ネットワークを介して配布する構成であっても良い。例えば、パソコンなどのネットワーク機能を有するクライアント機器にICカードが挿入されている場合、ICカードがパソコンのネットワーク機能を利用してAD内サーバと通信を行い、ネットワークを介して共通秘密情報を受取る

。

【００５０】

なお、前記ネットワークを用いた登録の最大数と、前記ICカードを用いた登録台数の最大数を、個々に決めてもよいし、合計の台数だけを制限する方法であってもよい。

以上のように、本発明では、共通秘密情報の配布方法を限定するものではなく、登録機器の台数、つまり配布した共通秘密情報の数を管理してその配布を制御し、共通秘密情報を持っているか否かでADを明確に規定する所にその特徴がある。

【００５１】

［AD内サーバにおける登録情報］

図3の登録情報記憶部221に記憶する登録情報とその制御について、以下説明する。

登録情報記憶部および制御部は、基本的にはADに登録するクライアントの台数を記憶して、予め定められた登録台数内なら共通秘密情報CSIの送付を許可する、予め定められた登録台数以上になった段階でCSIの送付を禁止するといった制御を行う。

【００５２】

例えば、登録の最大数と、現登録数、残りの登録数を記憶して制御する。登録の最大数は、予め機器に埋め込まれているか、登録台数制御機関を別途設けて、この機関が署名をつけて例えばDVDのような蓄積メディアや通信を介して安全に配布される。AD内サーバは、その情報が正しいことを確認のうえで、登録の最大数を記録する。

【００５３】

例えば、AD内サーバから上記登録台数制御機関に、登録したい台数を要求し、それに対する代金支払いをすれば、登録台数制御機構から、対応する情報が送られるという仕組みであってもよい。この場合、この対応する情報は、当該の料金支払いをしたAD内サーバにのみ設定できる。

また、現登録数は、それまでのクライアント登録の台数を記録し、新たなクラ

イアント機器を登録するたびに、＋１するものとする。

【００５４】

また、残りの登録数は、登録の最大数から現登録数を引いた値であり、新たなクライアント機器を登録するたびに、－１するものとする。登録制御部は、この値が０になったかどうかを確認し、０でなければ新たなクライアント機器を登録可能とし、０であれば、登録をせずに処理を中断するといった制御を行う。

なお、登録情報の中には、登録クライアント機器のID番号を記録してもよい。このことにより、すでに登録済みのクライアント機器が、間違えて再度登録を試みた場合、AD内サーバ側でID番号の照合により、CSIの照合より前に検知して、クライアント機器に通知し処理を中断することができる。

【００５５】

上記では、最大登録数を設定してその範囲での登録を許可していたが、もし、AD内サーバから上記登録台数制御機構に安全に登録台数の情報を送り、これに対応して課金する仕組みがあれば、AD内サーバでは登録台数だけを管理しておいてもよい。

なお、上記では、最大登録数、現登録数、残りの登録台数の３つの情報で管理をしていたが、これは例えば最大登録台数を初期値とし、残りの登録台数だけで管理してもよい。また、最大登録数と現登録数だけで管理をしてもよい。

【００５６】

[共通秘密情報]

AD内で共通に保有する共通秘密情報について説明する。この情報は容易に推測されたり、簡単に試すことが可能な値であってはならない。そのため、ある程度長いビット長のデータ（例えば200ビット程度）であることが必要である。

また、上記の例では、共通秘密情報CSIはAD内サーバが生成するとしている。この場合、各AD内サーバが任意に生成してAD内クライアントに登録と同時に配布する。これは２つのAD内サーバが独立にそれぞれCSIを生成しても、上記の通り長いビット長のデータであれば、それらが偶然にも同じになる確率が小さいであろうとの仮定に基づいている。

【００５７】

より厳密に各AD間のCSIの重複を回避するためには、例えば複数のAD内サーバ間で情報を交換して、重複しているかを確認をすればよい。CSIそのものを送付しあうことは、安全性が低下するため、その場合は、例えば決められたハッシュ関数を用いて、各CSIのハッシュ値（CSIをハッシュ関数に入力したときの出力）を交換して重複の有無を確認すればよい。ハッシュ関数は、出力のハッシュ値からその入力のCSIが求められないような関数である。この出力が一致している場合は、CSIそのものが一致している可能性が高いため、再度CSIを作り直せばよい。ハッシュ関数の例としてはSHA-1アルゴリズムを用いればよい。

【００５８】

また、別の実現例としては、１つの信頼の置ける機関が、集中して全ADのCSIを重複がないように生成し、これを安全に各AD内サーバに送付するという方法であってもよい。

[SAC]

次に、暗号通信が可能となる安全な通信路（SAC：Secure Authentication Channel）について、図６を用いて説明する。SACには２つのモードがある。

【００５９】

1つ目のモードは、AD内サーバがクライアント機器を登録する場合（図４におけるS302）に用いる。このモードでは、以下に述べる共通秘密情報CSI（Common Secret Information）を予め未登録クライアントに設定されている値とし、AD内サーバはこのSACにより、対象とするクライアント機器がCAに認められた正しい機器であることとともに、未登録クライアントであることを認証し、セッション鍵を共有する。

【００６０】

２つ目のSACのモードは、AD登録後に同じSAC内の機器であるかを確認するのに用いる。例えばAD登録後、コンテンツを配布する前に用いる。あるいは、ADから脱退する場合、その認証の際に用いる。このSACのモードでは、以下に述べる共通秘密情報CSIは、AD登録の際にAD内サーバとAD内クライアントが共有した共通秘密情報とする。AD内サーバでは、これにより、対象とするクライアント機器がCAに認められた正しい機器であることとともに、同じAD内であることを認証し、

セッション鍵を共有する。

【００６１】

図6では、上記２つ目のモードについて説明している。１つ目のモードについては、CSIの値が、未登録であることを示す予め決められた値であるという点を除けば、2つ目のモードと同じである。

ただし、Sign()を署名生成関数、Veri()を署名検証関数、Gen()を鍵生成関数とし、Yをそのシステム固有のシステムパラメータとする。また、鍵生成関数Gen()は、Gen(x,Gen(y,z)) = Gen(y,Gen(y,z))の関係を満たすものとする。なお、このような鍵生成関数は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、ディフィ-ヘルマン（DH）型公開鍵配送法がある（例えば、非特許文献４参照）。また、図６ではAD内サーバ101が計算あるいは生成するデータには、Aの添え字、クライアント機器111が計算あるいは生成するデータには、Bの添え字をつけて区別して表現している。

【００６２】

S701：AD内サーバは、CAが発行した証明書Cert#Aをクライアント機器に送信する。ここでは、証明書の構成要素は、AD内サーバの公開鍵PK#A、AD内サーバのID（ID#A）、それらに対するCAの署名Sig#CAとする。

S702：クライアント機器は、CAの公開鍵PK#CAを用いてCert#Aに付与されている署名Sig#CAが正しい否かを検証する。検証結果が正しくなければ、SACの確立処理を終了する。さらに、クライアント機器は、AD内サーバのID（ID#A）が証明書無効化リスト（CRL：Certification Revocation List）に登録されているか否かを確認する。登録されていれば、SACの確立処理を終了する。CRLは無効化されている機器のIDを一覧し、これにCAの署名が施されたデータである。CRLは、例えば機器が盗難されたり紛失したときに、機器のユーザからの要望でCRLにその機器のIDを載せて、不正に利用されることを防ぐなどの使い方をする。なお、各機器は、例えば放送やインターネット、またはDVDのようなパッケージメディアを用いて、最近のCRLを入手する。

【００６３】

S703：クライアント機器は、CAが発行した証明書Cert#BをAD内サーバに送信す

る。ここで、証明書の構成要素は上記同様とする。

S704：AD内サーバは、CAの公開鍵PK#CAを用いてCert#Bに付与されている署名Sig#CAが正しい否かを検証する。検証結果が正しくなければ、SACの確立処理を終了する。さらに、AD内サーバは、クライアント機器のID（ID#B）がCRLに登録されているか否かを確認する。登録されていれば、SACの確立処理を終了する。

【００６４】

S705：クライアント機器は、乱数Cha#Bを生成して、AD内サーバに送信する。

S706：AD内サーバは、受信したCha#Bに共通秘密情報CSIを連結して、自身の秘密鍵SK#Aで署名Sig#Aを生成して、クライアント機器に送信する。なお、一般的には署名対象となる情報のハッシュ値を計算し、これに対して署名する。

S707：クライアント機器は、S701で受信したAD内サーバの公開鍵PK#Aを用いて、さらに自身が保持している共通秘密情報CSIを用いてSig#Aが正しいか否かを検証する。検証結果が正しくなければ、対応する機器が認証されたものでない、あるいは同じAD内にないと判断し、SACの確立処理を終了する。この検証結果は、AD内サーバがCert#Aに対応した秘密鍵SK#Aを保持し、かつクライアント機器と同じ共通秘密情報CSIを保持している場合に限って正しいものになる。

【００６５】

S708：AD内サーバは、乱数Cha#Aを生成して、クライアント機器に送信する。

S709：クライアント機器は、受信したCha#Aに共通秘密情報CSIを連結して、自身の秘密鍵SK#Bで署名Sig#Bを生成して、AD内サーバに送信する。

S710：AD内サーバは、S703で受信したクライアント機器の公開鍵PK#Bを用いて、Sig#Bが正しいか否かを検証する。検証結果が正しくなければ、対応する機器が認証されたものでない、あるいは同じAD内にないと判断し、SACの確立処理を終了する。この検証結果は、クライアント機器がCert#Bに対応した秘密鍵SK#Bを保持し、かつAD内サーバと同じ共通秘密情報CSIを保持している場合に限って正しいものになる。

【００６６】

S711：AD内サーバは、乱数aを生成し、Key#A=Gen(a,Y)を計算してクライアント機器に送信する。

S712：クライアント機器は、乱数bを生成し、Key#B=Gen(b,Y)を計算してAD内サーバに送信する。さらに、両者で共有する鍵Key#AB = Gen(b,Key#A)を算出して、セッション鍵SK=Gen(CSI,Key#AB)を算出する。

【００６７】

S713：AD内サーバは、受信したKey#Bと、S711で生成した乱数aを用いて、共有する鍵Key#AB=Gen(a,Key#B)を算出して、セッション鍵SK = Gen(CSI,Key#AB)を算出する。

以上のように、チャレンジ／レスポンスを利用した相手認証処理に共通秘密情報が同じであることを確認する処理を追加することで、通信相手が正しい機器か否か、かつ、同じAD内に登録されている機器であるか否かを確実に判定することができる。

【００６８】

さらに、上記の方法はGen関数を用いたセッション鍵の生成にも、認証のチャレンジ／レスポンスと同様に、共通秘密情報を利用（作用）している。そのため、共通秘密情報を持つ相手とだけ、確実にセッション鍵を共有することが可能となる。

なお、本発明は上記構成に限定されるものではない。例えば、相手認証処理だけに共通秘密情報を利用したり、鍵共有処理だけに共通秘密情報を利用したりする構成であってもよい。また、上記構成では、双方向に認証を行っているが、片側認証であってもよい。

【００６９】

また、本発明における共通秘密情報の利用方法は、上記のように公開鍵暗号を利用した方法に限定されるものではない。例えば、共通秘密情報に乱数データを連結する構成ではなく、共通秘密情報と乱数データを加算する構成であってもよい。

このように、本発明では、SACの設定方法を限定するものではなく、SACの確立処理に共通秘密情報を作用させ、共通秘密情報を持つ相手とのみSACを確立して、コンテンツの送受信を行う所にその特徴がある。

【００７０】

＜ADからクライアント機器の脱退方法＞

次に、ADに登録しているクライアント機器が、そのADから脱退する方法について述べる。図７は、AD内サーバと同じ共通秘密情報CSIを有するクライアント機器111が、CSIを返却して、ADを脱退する場合のフローを示している。以下、その詳細について説明する。

【００７１】

S501：クライアント機器が、AD脱退要求を行う。

S502：AD内サーバとクライアント機器の間でSACを確立する。SACについては前述した2番目のモードを使用する。

S503：AD内サーバはクライアント機器が同じAD内にいることを認証する。もしなければ、AD内サーバはクライアント機器にその旨を通知して処理を中断する。

【００７２】

S504：AD内サーバはクライアント機器に共通に保持するCSI削除を通知する。この通知は、SACを利用して行われる。

S505：クライアント機器は対応するCSIを削除し、削除が完了したことをAD内サーバに通知する。

S506：AD内サーバは、登録情報にある前記クライアント機器の情報を削除し、現登録数を［－1」、残りの登録台数を「＋１」する。

【００７３】

以上のように、AD内サーバが、残りの登録数を「＋１」し、かつ、クライアント機器が自らのCSIを削除することで、ADに存在するクライアントの最大数を、予め定められた数で保つことが可能となる。

＜クライアント機器間でのCSIの移動方法＞

次に、すでにADに登録しているクライアント機器1が、AD未登録の別のクライアント機器2に、登録を入れ替わり、CSIを移動する方法について述べる。これは例えば機種変更を、クライアント機器のみで行う場合に使用される。以下、図８に従ってその詳細について説明する。

【００７４】

S801：クライアント機器2が、クライアント機器１にCSIの移動要求を行う。

S802：クライアント機器1とクライアント機器２の間でSACを確立する。ここでは、クライアント機器１はSACの第1のモードを用いてクライアント機器２が未登録であることを確かめる。

S803：クライアント機器２が登録済みである場合は、クライアント機器１はその旨をクライアント機器２に通知して、処理を中断する。

【００７５】

S804：クライアント機器１はSACで共有したセッション鍵を用いて、CSIをクライアント機器２に通知する。

S805：クライアント機器２はCSIを共通秘密情報格納部に保存する。

S806：クライアント機器2は、クライアント機器１にCSI保存完了を通知する。

S807：クライアント機器１は共通秘密情報記憶部から、CSIを削除する。

【００７６】

以上のように、クライアント機器２がCSIを保存し、クライアント機器１がCSIを削除することで、ADに存在するクライアントの最大数を、予め定められた数で保つことが可能となる。なお、クライアント機器１は、AD内サーバにCSIをクライアント機器２に移動した旨を通知してもよい。AD内サーバはこの情報をもとにして、登録情報を更新する。

【００７７】

なお、脱退したクライアント機器や、CSIの移動元のクライアント機器１が、他のAD内サーバ、あるいは再度同じAD内サーバに登録できるようにするためには、脱退時にクライアント機器の共通秘密情報格納部に、未登録であることを示す情報を蓄積するとよい。

＜AD内でのコンテンツ配信方法＞

AD内サーバ101から、クライアント機器111へコンテンツを送信する方法について以下に説明する。ここでは、コンテンツの蓄積形態は問わないが、一例として、コンテンツはコンテンツ鍵で暗号化されて、コンテンツ鍵は、AD内サーバを一意に識別する機器IDと、共通秘密情報から生成される鍵で暗号化されて、例えば、AD内サーバが持つハードディスクに記録されているものとする。この例では、コンテンツ鍵の暗号化にAD内サーバの機器IDを利用することで、その機器でのみ

コンテンツの利用が可能となる。

【００７８】

図９は、コンテンツ配信方法のフローを示している。以下、その詳細について説明する。

S601：AD内サーバ101とクライアント機器111の間で、共通秘密情報を用いたSACを確立する。ここでは、SACの2番目のモードを用いて、お互いに同じCSIを有していることを確認する。

【００７９】

S602：AD内サーバ101は、暗号化コンテンツ鍵を、共通秘密情報とAD内サーバ101の機器IDから生成した鍵で復号して、復号したコンテンツ鍵をS601で共有したセッション鍵で再暗号化する。

S603：AD内サーバ101は、S602で再暗号化した暗号化コンテンツ鍵と、暗号化コンテンツをクライアント機器111へ送信する。

【００８０】

S604：S603を受信したクライアント機器は、セッション鍵で暗号化コンテンツ鍵を復号してコンテンツ鍵を得る。

S605：クライアント機器が受信したコンテンツを蓄積する場合、S604で得たコンテンツ鍵を、共通秘密情報とクライアント機器の機器IDから生成する鍵で再暗号化して、暗号化コンテンツと共に、例えば、クライアント機器のハードディスクに蓄積する。

【００８１】

S606：クライアント機器が受信したコンテンツをその場で再生する場合、S604で得たコンテンツ鍵で暗号化コンテンツを復号して、コンテンツの再生を行う。

なお、上記ではAD内サーバとクライアント機器間でのコンテンツ配送について述べたが、クライアント間のコンテンツ配送であってもよい。共有する共通秘密情報を用いて同様に行うことができる。

【００８２】

また、ADに識別子を付与し、コンテンツ配信時にコンテンツ自身にADの識別子を電子透かしとして埋め込むようにしてもよい。これにより、クライアント機器

が復号したあとのコンテンツを、不正にAD外に配布した場合に、そのコンテンツがどこのADから流出したのかを特定することができる。さらに、もしコンテンツを配信するサーバが、各ADに登録しているクライアント機器を管理している場合、そのADに属するクライアント機器でのコンテンツの再生を禁止するための、CRLに載せてもよい。

【００８３】

＜時間で制御＞

なお、以上の説明におけるクライアント機器の登録やCSIの移動を、時間制限された仮のものであってもよい。例えば、登録の場合の手順は次のとおりである。

(1) まず、AD内サーバとクライアント機器の間で時間を合わせ、かつ有効期限を定める。

【００８４】

(2) AD内サーバにクライアント機器を登録する。これに従って、AD内サーバ内の残りの登録台数は「－1」となる。クライアント機器にはCSI情報が伝えられる。

(3) 定められた時刻になったら、クライアント機器からCSI情報が自動的に削除される。また、AD内サーバからもクライアント機器の登録情報は削除され、残り登録台数が「＋１」され、もとの状態にもどる。

【００８５】

＜複数AD内サーバの場合＞

なお、以上の説明においては１つのAD内にAD内サーバは複数あってもよい。この場合、クライアント機器はいずれのAD内サーバとやり取りをすればよいのかを、決めることができる。この決め方としては、例えばユーザが設定するのでもよいし、機器がAD内で距離が近いものを自動的に選択する方法であってよい。あるいは、AD内サーバのうち、処理能力が高いものや、他のタスクが少ないほうをクライアント機器が自動で選んでもよい。

【００８６】

＜複数AD間の関係＞

なお、複数のAD間で、登録されているクライアント機器のリスト情報を交換することにより、あるクライアント機器がどのADに属しているのか、あるいは、いくつのADに属しているのかを知ることができる。このことにより、1台のクライアント機器が属するAD数を限定することもできる。例えば1台の機器は１つのADにのみ属するという場合には、その重複を検知することもできる。

【００８７】

クライアント機器は複数のADに登録できるようにしてもよい。このとき、クライアント機器内で登録するADの個数を制限する構成であってもよい。また、クライアント機器が属する複数ADの各AD内サーバが情報を交換して、１つのクライアント機器が登録しているADの個数を制限する攻勢であってもよい。また、クライアント機器が登録するADの個数を管理する機関を、別途設けてもよい。

【００８８】

（その他の変形例）

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

（１）上記の各装置は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、各装置は、その機能を達成する。

【００８９】

（２）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂ

ｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【００９０】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【００９１】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（３）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【００９２】

【発明の効果】

以上のように、本発明によれば、コンテンツの利用、コピー等を可能とする許可された範囲（AD）を、AD内サーバの登録クライアント台数で制限する。AD内サーバは、AD内のクライアント台数を管理し、この範囲でのコンテンツの利用、コピー等を可能とする。また、AD内の機器の登録や脱退、機器の変更を可能とする。

【００９３】

AD内の登録機器台数は、予め外部より設定されていたり、課金に依存することもできる。また、AD内サーバとオンライン接続されていない機器（例えば車載機器など）も、ICカードのように着脱可能なセキュアデバイスを用いてAD内クライアントとして登録が可能である。

【図面の簡単な説明】

【図１】

ADの概念図

【図２】

AD登録の概念図

【図３】

AD登録の内部構成図（ネットワーク利用）

【図４】

AD登録時の処理フローチャート

【図５】

AD登録時の内部構成図（ICカード利用）

【図６】

SACの処理フローチャート

【図７】

AD脱退時の処理フローチャート

【図８】

CSI移動時の処理フローチャート

【図９】

AD内のコンテンツの配送フローチャート

【符号の説明】

１０１…AD内サーバ

１１１、１１２…AD内クライアント

１２０…AD外クライアント

２０１、２４１、４０１…公開鍵証明書格納部

２０２、２４２、４０２…秘密鍵格納部

２０３、２４３、４０３…公開鍵暗号処理部

２１１…共通秘密情報生成部

２１２、２５１、４１１…共通秘密情報格納部

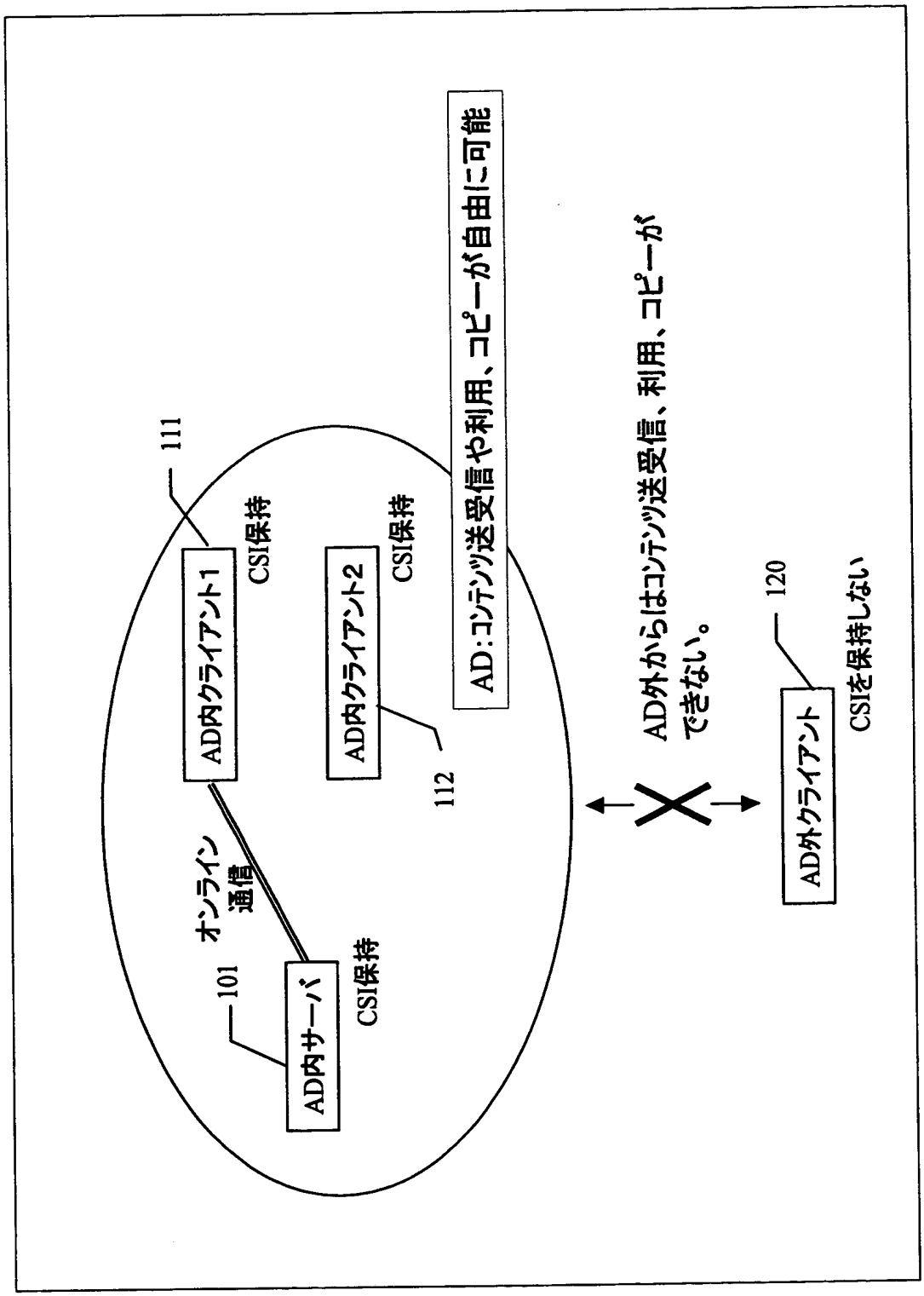
２２１…登録情報記憶部

２２２…登録制御部

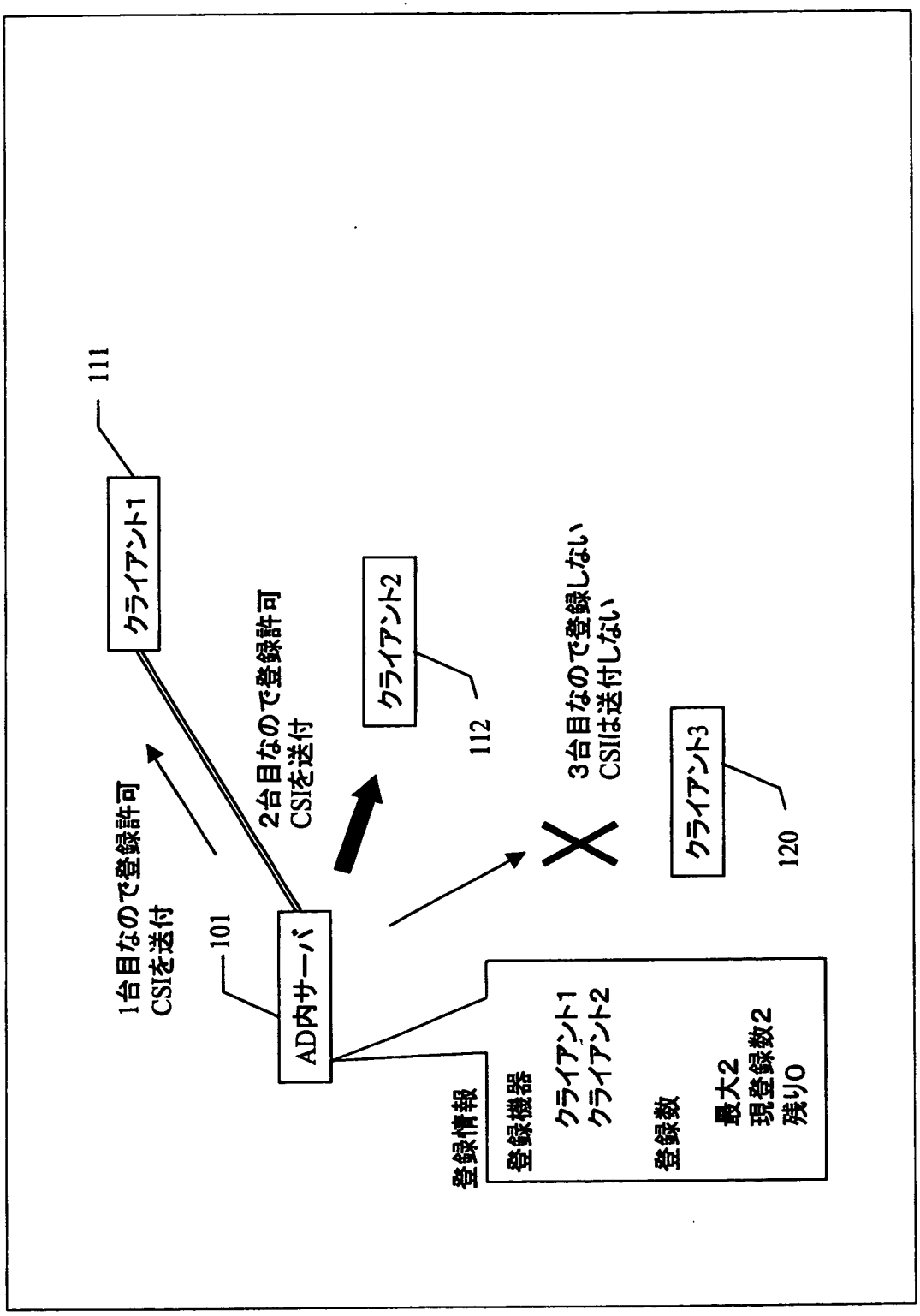
２３１、２６１４２１…入出力部

【書類名】　　図面

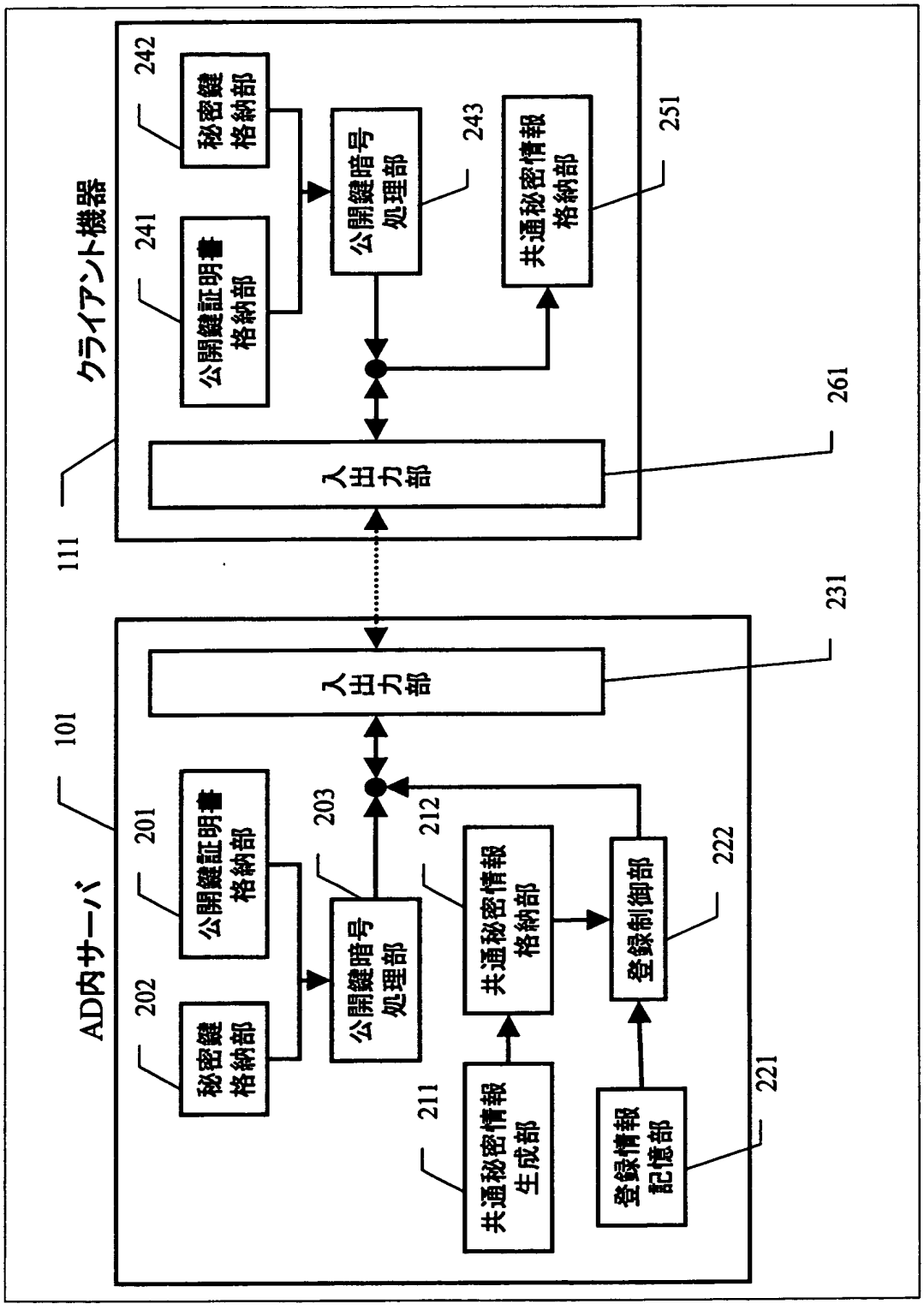
【図１】


AD:コンテンツ送受信や利用、コピーが自由に可能
111
AD内クライアント1
CSI保持
AD内クライアント2
CSI保持
112
オンライン
通信
101
AD内サーバ
CSI保持
AD外からはコンテンツ送受信、利用、コピーが
できない。
120
AD外クライアント
CSIを保持しない

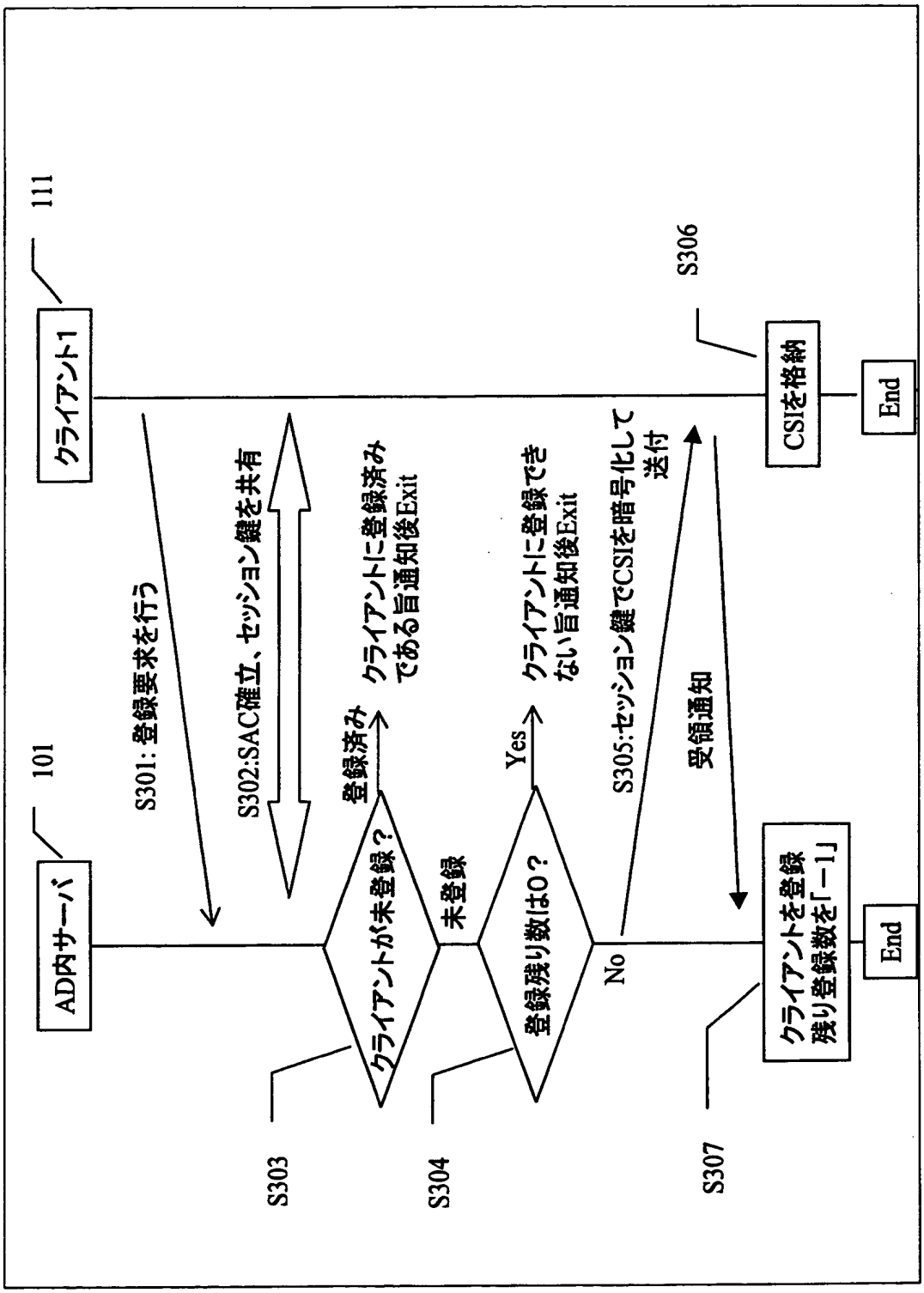
【図２】


111
クライアント1
2台目なので登録許可
CSIを送付
クライアント2
112
3台目なので登録しない
CSIは送付しない
クライアント3
120
1台目なので登録許可
CSIを送付
101
AD内サーバ
登録情報
登録機器
クライアント1
クライアント2
登録数
最大2
現登録数2
残り0

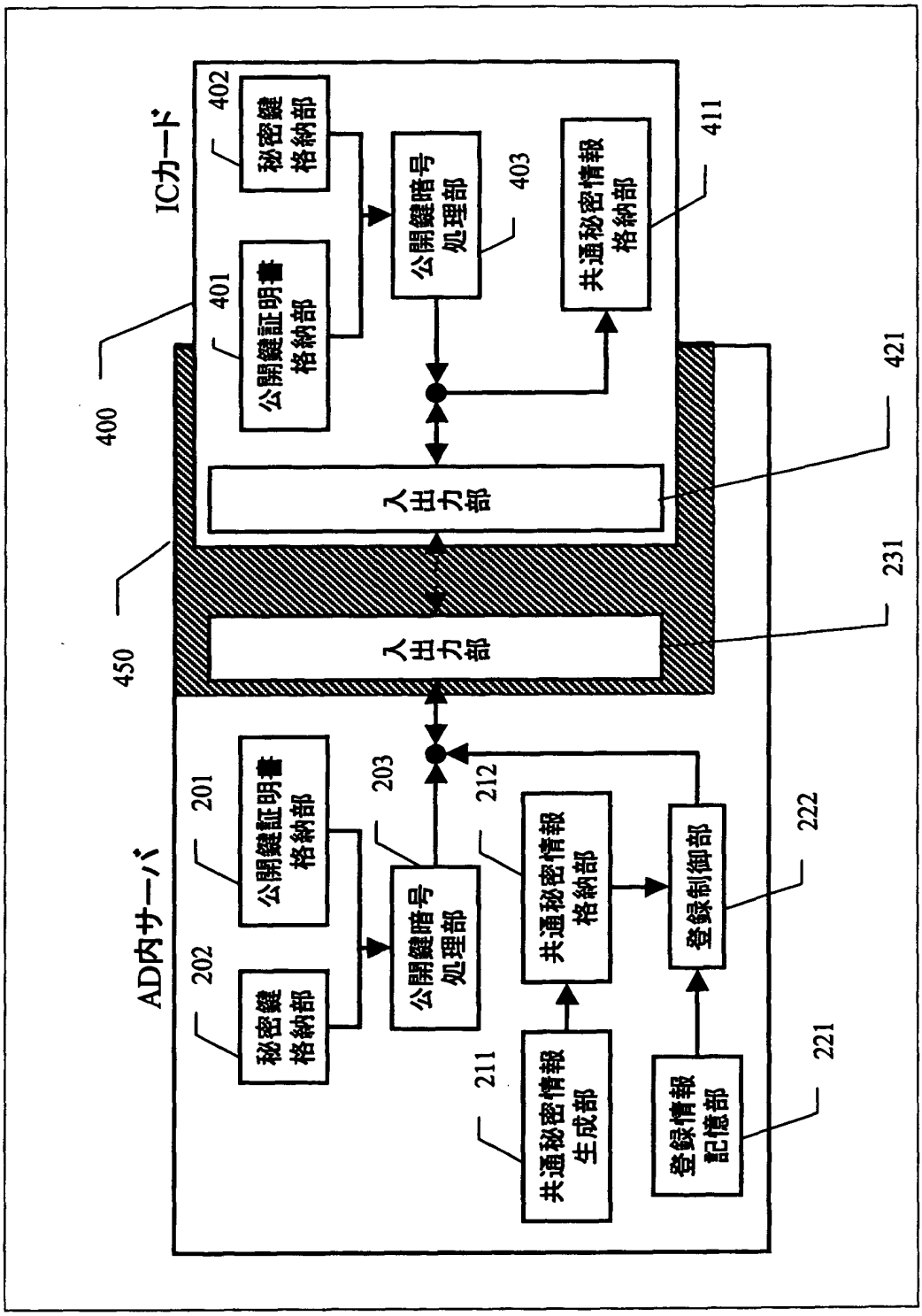
【図３】


クライアント機器
111
242
秘密鍵格納部
241
公開鍵証明書格納部
243
公開鍵暗号処理部
251
共通秘密情報格納部
261
入出力部
AD内サーバ
101
231
入出力部
201
公開鍵証明書格納部
202
秘密鍵格納部
203
公開鍵暗号処理部
212
共通秘密情報格納部
222
登録制御部
211
共通秘密情報生成部
221
登録情報記憶部

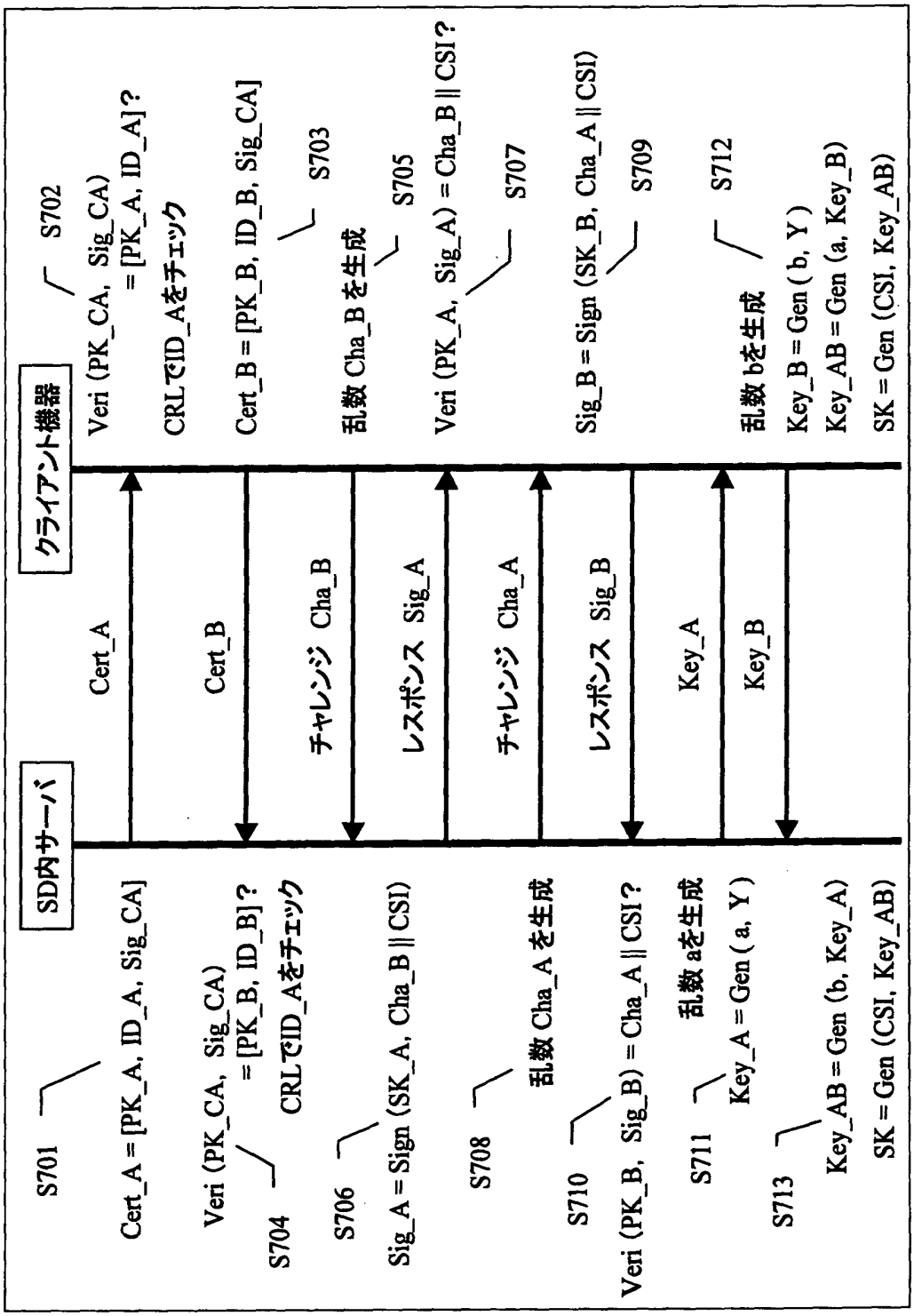
【図４】


AD内サーバ
101
クライアント1
111
S301: 登録要求を行う
S302:SAC確立、セッション鍵を共有
S303
クライアントが未登録？
登録済み
クライアントに登録済み
である旨通知後Exit
未登録
S304
登録残り数は0？
Yes
クライアントに登録でき
ない旨通知後Exit
No
S305:セッション鍵でCSIを暗号化して
送付
S306
CSIを格納
End
受領通知
S307
クライアントを登録
残り登録数を「－1」
End

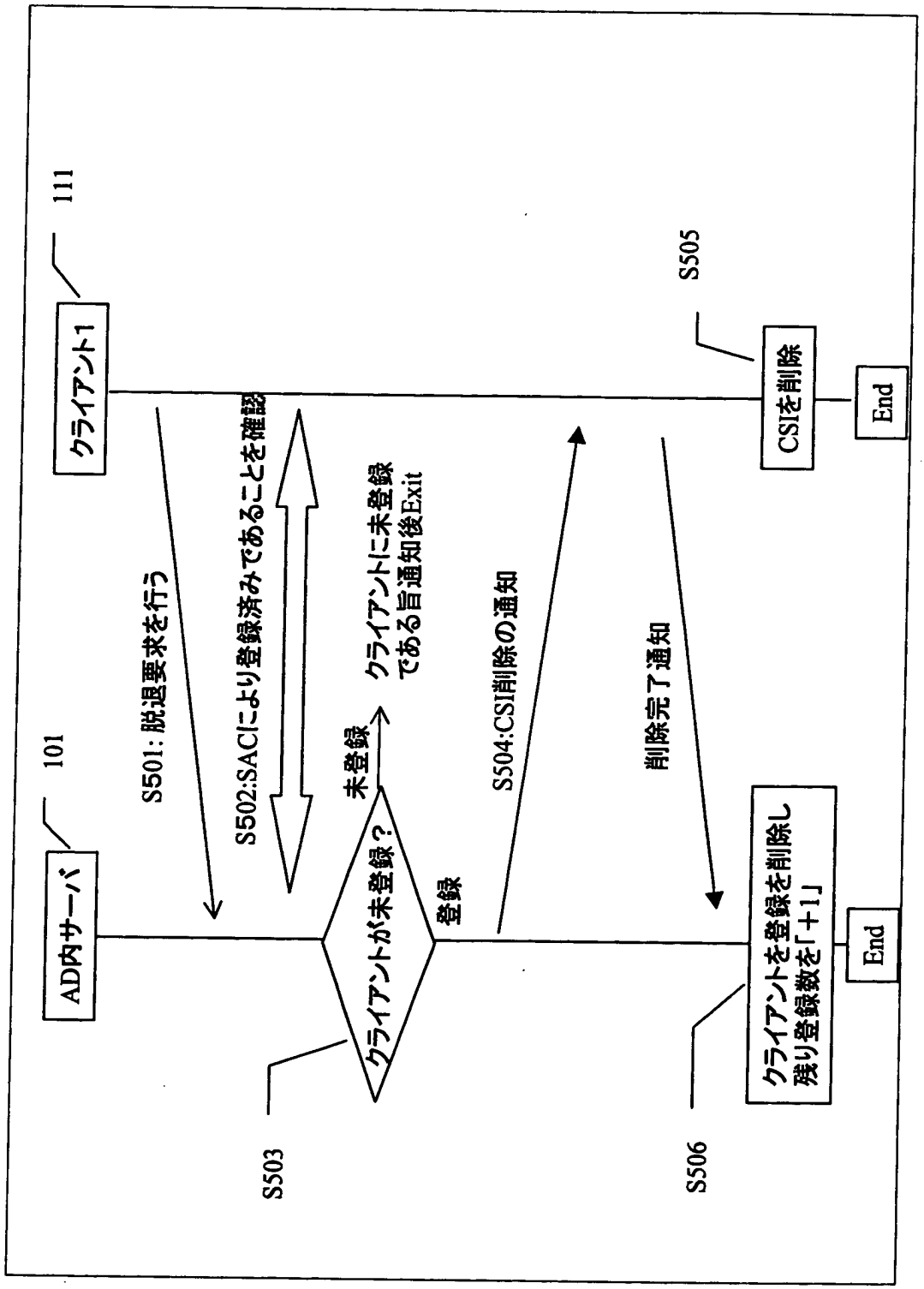
【図５】


ICカード
400
秘密鍵格納部
402
公開鍵証明書格納部
401
公開鍵暗号処理部
403
共通秘密情報格納部
411
入出力部
421
450
入出力部
231
AD内サーバ
公開鍵証明書格納部
201
秘密鍵格納部
202
公開鍵暗号処理部
203
212
共通秘密情報格納部
登録制御部
222
共通秘密情報生成部
211
登録情報記憶部
221

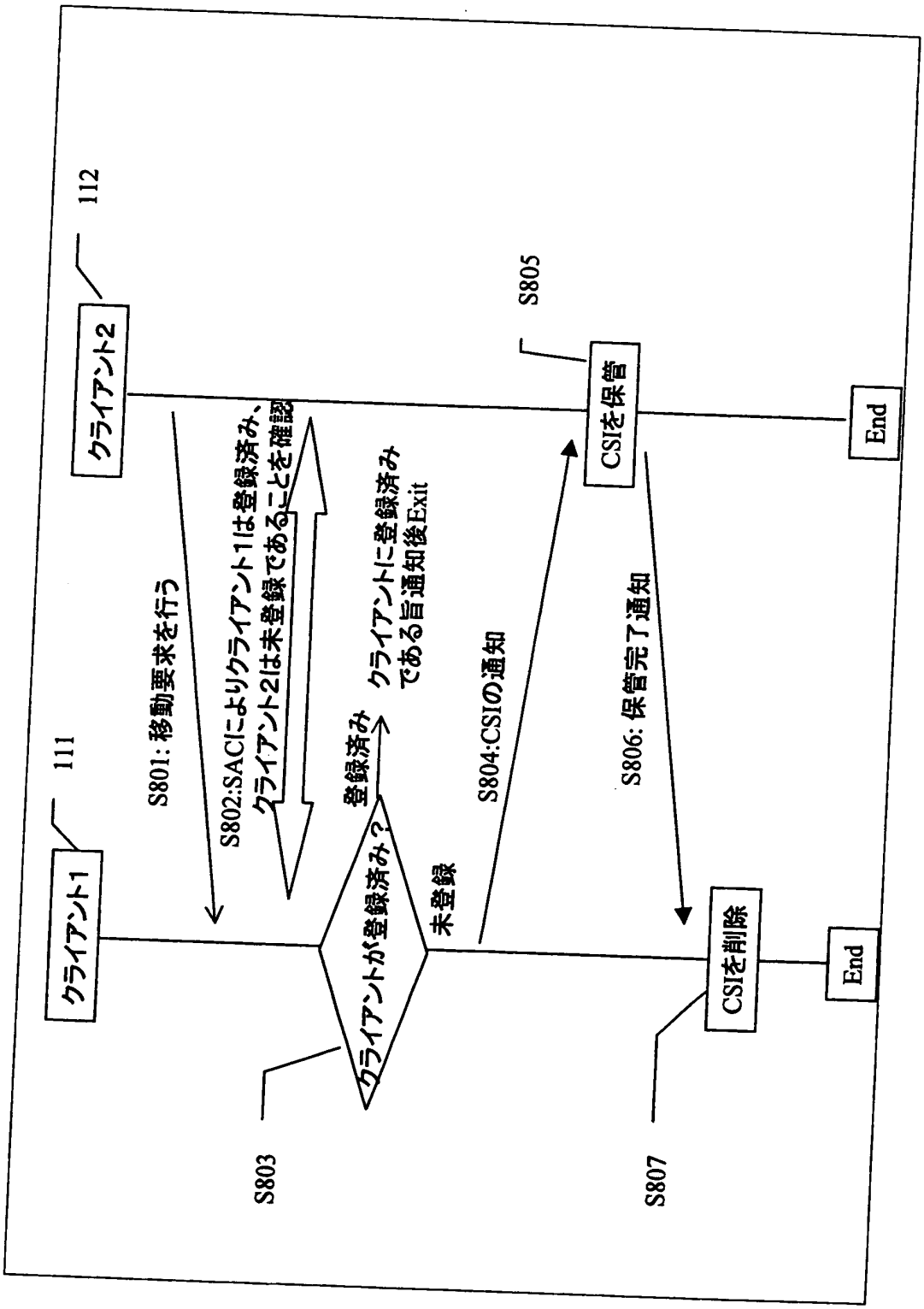
【図６】


SD内サーバ
クライアント機器
S701
Cert_A = [PK_A, ID_A, Sig_CA]
Cert_A
S702
Veri (PK_CA, Sig_CA) = [PK_A, ID_A]?
CRLでID_Aをチェック
Cert_B
Cert_B = [PK_B, ID_B, Sig_CA]
S703
乱数 Cha_B を生成
チャレンジ Cha_B
S704
Veri (PK_CA, Sig_CA) = [PK_B, ID_B]?
CRLでID_Aをチェック
S705
Veri (PK_A, Sig_A) = Cha_B || CSI?
レスポンス Sig_A
S706
Sig_A = Sign (SK_A, Cha_B || CSI)
S707
乱数 Cha_A を生成
チャレンジ Cha_A
S708
Sig_B = Sign (SK_B, Cha_A || CSI)
S709
Veri (PK_B, Sig_B) = Cha_A || CSI?
レスポンス Sig_B
S710
Key_A
S711
乱数 aを生成
Key_A = Gen (a, Y)
S712
乱数 bを生成
Key_B
S713
Key_B = Gen (b, Y)
Key_AB = Gen (b, Key_A)
Key_AB = Gen (a, Key_B)
SK = Gen (CSI, Key_AB)
SK = Gen (CSI, Key_AB)

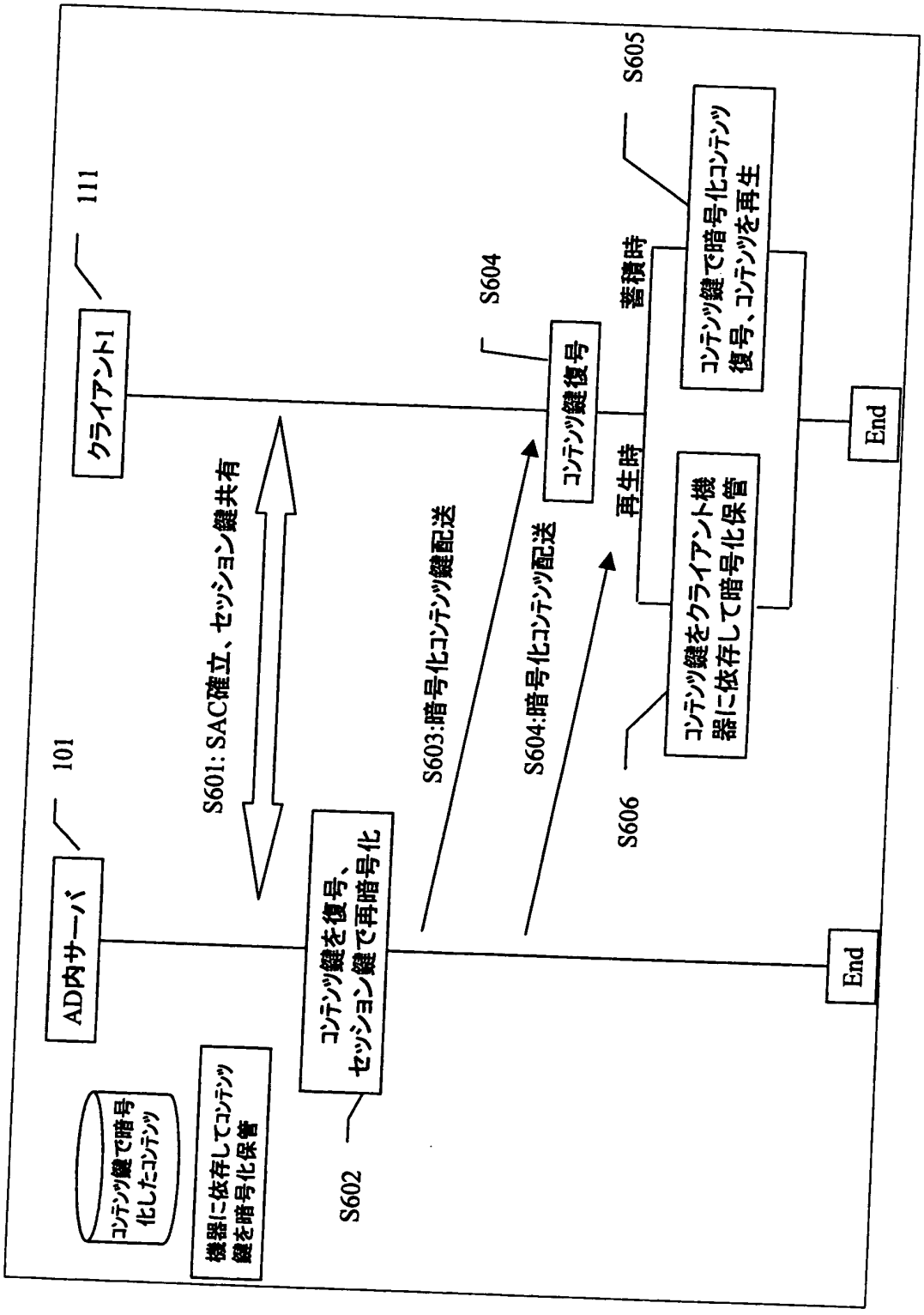
【図７】


111
クライアント1
101
AD内サーバ
S501: 脱退要求を行う
S502:SACにより登録済みであることを確認
未登録
クライアントに未登録
である旨通知後Exit
クライアントが未登録？
登録
S503
S504:CSI削除の通知
削除完了通知
S505
CSIを削除
End
S506
クライアントを登録を削除し
残り登録数を「+1」
End

【図８】


112
クライアント2
S805
CSIを保管
End
S801: 移動要求を行う
S802:SACによりクライアント1は登録済み、クライアント2は未登録であることを確認
登録済み
クライアントに登録済みである旨通知後Exit
S804:CSIの通知
S806: 保管完了通知
111
クライアント1
クライアントが登録済み？
未登録
CSIを削除
End
S803
S807

【図９】


AD内サーバ
101
クライアント1
111
S601: SAC確立、セッション鍵共有
コンテンツ鍵で暗号化したコンテンツ
機器に依存してコンテンツ鍵を暗号化保管
コンテンツ鍵を復号、セッション鍵で再暗号化
S602
S603:暗号化コンテンツ鍵配送
S604:暗号化コンテンツ配送
コンテンツ鍵復号
S604
蓄積時
再生時
S605
コンテンツ鍵で暗号化コンテンツ復号、コンテンツを再生
コンテンツ鍵をクライアント機器に依存して暗号化保管
S606
End
End

【書類名】　要約書

【要約】

【課題】ディジタルコンテンツ著作権保護の観点より、無制限なコピーや移動は許可されない。一方、ユーザは、私的利用の範囲に限定して自由なコピーや移動を可能にしたい。

【解決手段】私的利用の範囲を台数制限で管理し、コンテンツをその範囲にバインドしてコピーや移動する。私的利用の範囲をネットワークやセキュアデバイスを用いて登録する。

【選択図】図１

出願人履歴情報

識別番号　〔０００００５８２１〕

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社